



## Calhoun: The NPS Institutional Archive

---

Faculty and Researcher Publications

Faculty and Researcher Publications Collection

---

2015-08-05

# On weak and strong 2k-bent Boolean functions

Stănică, Pantelimon

---

<http://hdl.handle.net/10945/48930>



Calhoun is a project of the Dudley Knox Library at NPS, furthering the precepts and goals of open government and government transparency. All information contained herein has been approved for release by the NPS Public Affairs Officer.

**Dudley Knox Library / Naval Postgraduate School**  
**411 Dyer Road / 1 University Circle**  
**Monterey, California USA 93943**

<http://www.nps.edu/library>

# On weak and strong $2^k$ -bent Boolean functions

Pantelimon Stănică

Department of Applied Mathematics  
Naval Postgraduate School  
Monterey, CA 93943-5212, U.S.A.;  
Email: [pstanica@nps.edu](mailto:pstanica@nps.edu)

August 5, 2015

## Abstract

In this paper we introduce a sequence of discrete Fourier transforms and define new versions of bent functions, which we shall call (weak, strong) octa/hexa/ $2^k$ -bent functions. We investigate relationships between these classes and completely characterize the octabent and hexabent functions in terms of bent functions.

**Keywords:** Boolean functions, Walsh-Hadamard transforms, bent, negabent, octabent, hexabent functions.

## 1 Introduction

Let  $\mathbb{F}_2$  be the prime field of characteristic 2 and let  $\mathbb{V}_n := \mathbb{F}_2^n$  is the  $n$ -dimensional vector space over  $\mathbb{F}_2$ . A function from  $\mathbb{F}_2^n$  to  $\mathbb{F}_2$  is called a *Boolean function* on  $n$  variables. We denote the set of all Boolean functions by  $\mathcal{B}_n$ .

The set of integers, real numbers and complex numbers are denoted by  $\mathbb{Z}$ ,  $\mathbb{R}$  and  $\mathbb{C}$  respectively. The addition over  $\mathbb{Z}$ ,  $\mathbb{R}$  and  $\mathbb{C}$  is denoted by '+'. The addition over  $\mathbb{V}_n$  for all  $n \geq 1$ , is denoted by  $\oplus$ . If  $\mathbf{x} = (x_1, \dots, x_n)$  and  $\mathbf{y} = (y_1, \dots, y_n)$  are two elements of  $\mathbb{V}_n$  we define the scalar (or inner) product, by

$$\mathbf{x} \cdot \mathbf{y} = x_1 y_1 \oplus x_2 y_2 \oplus \dots \oplus x_n y_n.$$

We define the *scalar/inner product*  $\mathbf{x} \odot \mathbf{y}$  in  $\mathbb{C} \times \mathbb{C}$  in the same way, although the sum is over  $\mathbb{C}$ . We define the *intersection* of two vectors  $\mathbf{x}, \mathbf{y}$  in some vector space by

$$\mathbf{x} \star \mathbf{y} = (x_1 y_1, x_2 y_2, \dots, x_n y_n).$$

If  $z = a + bi \in \mathbb{C}$ , then  $|z| = \sqrt{a^2 + b^2}$  denotes the absolute value of  $z$ , and  $\bar{z} = a - bi$  denotes the complex conjugate of  $z$ , where  $i^2 = -1$ , and  $a, b \in \mathbb{R}$ .

An important tool in the analysis of Boolean functions is the discrete Fourier transform, known in Boolean function literature, as Walsh, Hadamard, or *Walsh-Hadamard transform*, which we define next

$$\mathcal{W}_f(\mathbf{u}) = 2^{-\frac{n}{2}} \sum_{\mathbf{x} \in \mathbb{V}_n} (-1)^{f(\mathbf{x}) \oplus \mathbf{u} \cdot \mathbf{x}}.$$

Any  $f \in \mathcal{B}_n$  can be expressed in *algebraic normal form* (ANF) as

$$f(x_1, x_2, \dots, x_n) = \bigoplus_{\mathbf{a}=(a_1, \dots, a_n) \in \mathbb{V}_n} c_{\mathbf{a}} \left( \prod_{i=1}^n x_i^{a_i} \right), \quad c_{\mathbf{a}} \in \mathbb{F}_2.$$

The character (sign) form of some binary vector  $\mathbf{x} = (x_1, \dots, x_n)$  is  $(-1)^{\mathbf{x}} = ((-1)^{x_1}, \dots, (-1)^{x_n})$ . The character form of a function is the character form of its truth table (output values). The (*Hamming*) *weight* of  $\mathbf{x} \in \mathbb{V}_n$  is  $\text{wt}(\mathbf{x}) := \sum_{i=1}^n x_i$ . The algebraic degree of  $f$ ,  $\deg(f) := \max_{\mathbf{a} \in \mathbb{V}_n} \{\text{wt}(\mathbf{a}) : c_{\mathbf{a}} \neq 0\}$ . Boolean functions having algebraic degree at most 1 are said to be *affine functions*. For any two functions  $f, g \in \mathcal{B}_n$ , we define the (*Hamming*) *distance*  $d(f, g) = |\{\mathbf{x} : f(\mathbf{x}) \neq g(\mathbf{x}), \mathbf{x} \in \mathbb{F}_2^n\}| = \text{wt}(f \oplus g)$ .

The maximum nonlinearity of a Boolean function  $f \in \mathcal{B}_n$  defined by  $nl(f) = \max\{d(f, \ell) \mid \ell \in \mathcal{A}_n, \text{ the affine functions in } n \text{ variables}\}$  known to be equal to  $nl(f) = 2^{n-1} - \frac{1}{2} \max_{\mathbf{u}} |\mathcal{W}_f(\mathbf{u})|$  is achieved when the maximum absolute value in the Walsh spectrum is minimized. For even  $n$ , such functions are known as *bent functions* [10] and the magnitudes of all the Walsh values in the spectrum is constant, that is, if  $|\mathcal{W}_f(\mathbf{u})| = 1$  for all  $\mathbf{u} \in \mathbb{V}_n$ . If  $f$  is bent, then for every  $\mathbf{u} \in \mathbb{V}_n$ , we have  $\mathcal{W}_f(\mathbf{u}) = \pm 1 = (-1)^{g(\mathbf{u})}$ , for some function  $g$ , which is also bent and called the *dual* of  $f$ . A function  $f \in \mathcal{B}_n$  is called *semibent*, if the Walsh transform of  $f$  takes the values  $\{0, \pm\sqrt{2}\}$ , when  $n$  is odd, or  $\{0, \pm 2\}$ , when  $n$  is even.

The sum  $\mathcal{C}_{f,g}(\mathbf{z}) = \sum_{\mathbf{x} \in \mathbb{V}_n} (-1)^{f(\mathbf{x}) \oplus g(\mathbf{x} \oplus \mathbf{z})}$  is the *crosscorrelation* of  $f$  and  $g$  at  $\mathbf{z}$ . The *autocorrelation* of  $f \in \mathcal{B}_n$  at  $\mathbf{u} \in \mathbb{V}_n$  is  $\mathcal{C}_{f,f}(\mathbf{u})$  above, which we denote by  $\mathcal{C}_f(\mathbf{u})$ . It is known [3] that a function  $f \in \mathcal{B}_n$  is bent if and only if  $\mathcal{C}_f(\mathbf{u}) = 0$  for all  $\mathbf{u} \neq 0$ .

We refer to Carlet [1, 2], and Cusick and Stănică [3] for more on Boolean functions.

Another transformation on Boolean functions was introduced by Rierra and Parker [9] (see also [7, 11]), and dubbed *nega-Hadamard transform* of  $f \in \mathbb{V}_n$  at any vector  $\mathbf{u} \in \mathbb{V}_n$  as the complex valued function  $\mathcal{N}_f(\mathbf{u}) = 2^{-\frac{n}{2}} \sum_{\mathbf{x} \in \mathbb{V}_n} (-1)^{f(\mathbf{x}) \oplus \mathbf{u} \cdot \mathbf{x}} i^{\text{wt}(\mathbf{x})}$ . A function is said to be *negabent* if the nega-Hadamard transform is flat in absolute value, namely  $|\mathcal{N}_f(\mathbf{u})| = 1$  for all  $\mathbf{u} \in \mathbb{V}_n$ . The sum  $C_{f,g}(\mathbf{z}) = \sum_{\mathbf{x} \in \mathbb{V}_n} (-1)^{f(\mathbf{x}) + g(\mathbf{x} \oplus \mathbf{z})} (-1)^{\mathbf{x} \cdot \mathbf{z}}$  is the *negacrosscorrelation* of  $f$  and  $g$  at  $\mathbf{z}$ , and the *negautocorrelation* of  $f$  at  $\mathbf{u} \in \mathbb{V}_n$  is  $C_f(\mathbf{u}) = \sum_{\mathbf{x} \in \mathbb{V}_n} (-1)^{f(\mathbf{x}) \oplus f(\mathbf{x} \oplus \mathbf{u})} (-1)^{\mathbf{x} \cdot \mathbf{u}}$ .

Let  $\zeta_{2^k} = e^{\frac{2\pi i}{2^k}}$  be a  $2^k$ -complex root of 1. In this paper we introduce yet an entire sequence of transforms, which we call  $2^k$ -Hadamard transform as the complex valued function

$$\mathcal{H}_f^{(2^k)}(\mathbf{u}) = 2^{-\frac{n}{2}} \sum_{\mathbf{x} \in \mathbb{V}_n} (-1)^{f(\mathbf{x}) \oplus \mathbf{u} \cdot \mathbf{x}} \zeta_{2^k}^{\text{wt}(\mathbf{x})}.$$

Certainly, if  $k = 1, 2$ , and so,  $\zeta_2 = -1, \zeta_4 = i$ , we get the Walsh-Hadamard, respectively, the nega-Hadamard transforms. If  $k = 3, 4$ , and so,  $\zeta_8 = e^{\frac{2\pi i}{8}} = \frac{1+i}{\sqrt{2}}$ ,  $\zeta_{16} = e^{\frac{2\pi i}{16}} = \frac{\sqrt{2}+\sqrt{2}i}{2} + i\frac{\sqrt{2}-\sqrt{2}i}{2}$ , then we shall call the corresponding transforms, the *octa-Hadamard transform*, respectively, *hexa-Hadamard transform* and denote them by  $\mathcal{O}_f(\mathbf{u})$ , respectively,  $\mathcal{X}_f(\mathbf{u})$ .

The  $2^k$ -crosscorrelation of  $f, g$ , respectively,  $2^k$ -autocorrelation of  $f$  are defined by

$$\begin{aligned} \mathcal{C}_{f,g}^{(2^k)}(\mathbf{u}) &= \sum_{\mathbf{x} \in \mathbb{V}_n} (-1)^{f(\mathbf{x}) \oplus g(\mathbf{x} \oplus \mathbf{z})} \mu^{\mathbf{x} \odot \mathbf{z}}, \\ \mathcal{C}_f^{(2^k)}(\mathbf{u}) &= \sum_{\mathbf{x} \in \mathbb{V}_n} (-1)^{f(\mathbf{x}) \oplus f(\mathbf{x} \oplus \mathbf{z})} \mu^{\mathbf{x} \odot \mathbf{z}}, \end{aligned}$$

where  $\mu = \zeta^2$  is a  $2^{k-1}$  complex root of 1 (recall the scalar product  $\mathbf{x} \odot \mathbf{z}$  is computed over  $\mathbb{Z}$ ). When  $k$  is fixed we shall use  $\mathcal{C}_{f,g}, \mathcal{C}_f$ , instead.

We call a function *octabent*, *hexabent*, and in general  $2^k$ -bent if and only if the octa-Hadamard, hexa-Hadamard, respectively,  $2^k$ -Hadamard transform are flat in absolute value, that is,  $|\mathcal{O}_f(\mathbf{u})| = 1$ ,  $|\mathcal{X}_f(\mathbf{u})| = 1$ ,  $|\mathcal{H}_f^{(2^k)}(\mathbf{u})| = 1$ , for all  $\mathbf{u} \in \mathbb{V}_n$ . Since it is relevant below, we call a function  $g$  a *strong*  $2^k$ -bent function if and only if  $g$  is  $2^\ell$ -bent for all  $\ell \leq k$ . Also, a function  $f$  is a *weak*  $2^k$ -bent function if and only if  $f \oplus s_{2^{k-1}}$  is a strong  $2^{k-1}$ -bent function.

In this paper, we will give some of the properties of the transform and we will investigate functions that are both bent, octabent, hexabent and

in general  $2^k$ -bent. In the case of octabent and hexabent, we will find a necessary and sufficient condition in terms of “lower-ladder” level of such functions.

## 2 Properties of the $2^k$ -Hadamard transform

Certainly, such transforms to be of any use, they have to be invertible.

**Lemma 1.** *Let  $f \in \mathcal{B}_n$ . Then*

$$(-1)^{f(\mathbf{y})} = 2^{-\frac{n}{2}} \zeta_{2^k}^{-\text{wt}(\mathbf{y})} \sum_{\mathbf{u} \in \mathbb{V}_n} \mathcal{H}_f^{(2^k)}(\mathbf{u}) (-1)^{\mathbf{y} \cdot \mathbf{u}}. \quad (1)$$

*Proof.* We have (let  $\delta_{\mathbf{0}}(\mathbf{x})$  be the Dirac symbol, which is 1 at  $\mathbf{x} = \mathbf{0}$  and 0, elsewhere),

$$\begin{aligned} 2^{-\frac{n}{2}} \sum_{\mathbf{u} \in \mathbb{V}_n} \mathcal{H}_f^{(2^k)}(\mathbf{u}) (-1)^{\mathbf{y} \cdot \mathbf{u}} &= 2^{-n} \sum_{\mathbf{u} \in \mathbb{V}_n} \sum_{\mathbf{x} \in \mathbb{V}_n} (-1)^{f(\mathbf{x}) \oplus \mathbf{u} \cdot \mathbf{x}} \zeta_{2^k}^{\text{wt}(\mathbf{x})} (-1)^{\mathbf{y} \cdot \mathbf{u}} \\ &= 2^{-n} \sum_{\mathbf{x} \in \mathbb{V}_n} \sum_{\mathbf{u} \in \mathbb{V}_n} (-1)^{f(\mathbf{x}) \oplus \mathbf{u} \cdot \mathbf{x}} \zeta_{2^k}^{\text{wt}(\mathbf{x})} (-1)^{\mathbf{y} \cdot \mathbf{u}} \\ &= 2^{-n} \sum_{\mathbf{x} \in \mathbb{V}_n} (-1)^{f(\mathbf{x})} \zeta_{2^k}^{\text{wt}(\mathbf{x})} \sum_{\mathbf{u} \in \mathbb{V}_n} (-1)^{\mathbf{u} \cdot (\mathbf{x} \oplus \mathbf{y})} \\ &= 2^{-n} \sum_{\mathbf{x} \in \mathbb{V}_n} (-1)^{f(\mathbf{x})} \zeta_{2^k}^{\text{wt}(\mathbf{x})} 2^n \delta_{\mathbf{0}}(\mathbf{x} \oplus \mathbf{y}) \\ &= (-1)^{f(\mathbf{y})} \zeta_{2^k}^{\text{wt}(\mathbf{y})}, \end{aligned}$$

and the lemma is shown.  $\square$

As in [11], we next prove a theorem that gives the  $2^k$ -Hadamard transform of various combinations of Boolean functions. For easy writing, when  $k$  is fixed, we shall use  $\mathcal{H}_f$  instead of  $\mathcal{H}_f^{(2^k)}$ . We will make use throughout of the well-known identity (see [5])

$$\text{wt}(\mathbf{x} \oplus \mathbf{y}) = \text{wt}(\mathbf{x}) + \text{wt}(\mathbf{y}) - 2\text{wt}(\mathbf{x} \star \mathbf{y}). \quad (2)$$

**Theorem 2.** *Let  $f, g, h$  be in  $\mathcal{B}_n$ ,  $\zeta = e^{\frac{2\pi i}{2^k}}$  and  $\omega = e^{\frac{\pi i}{2^k}}$  a square root of  $\zeta$ . The following statements are true:*

- (i) *If  $\ell_{\mathbf{a},c}(\mathbf{x}) = \mathbf{a} \cdot \mathbf{x} \oplus c$  is affine ( $\mathbf{a} \in \mathbb{V}_n, c \in \mathbb{F}_2$ ), then  $\mathcal{H}_{f \oplus \ell_{\mathbf{a},c}}(\mathbf{u}) = (-1)^c \mathcal{H}_f(\mathbf{a} \oplus \mathbf{u})$ . Moreover,*

$$\mathcal{H}_{\ell_{\mathbf{a},c}}(\mathbf{u}) = (-1)^c 2^n \left( \cos\left(\frac{\pi}{2^k}\right) \right)^n \left( -i \tan\left(\frac{\pi}{2^k}\right) \right)^{\text{wt}(\mathbf{a} \oplus \mathbf{u})} \omega^{n-2\text{wt}(\mathbf{a} \oplus \mathbf{u})}.$$

(ii) If  $h(\mathbf{x}) = f(\mathbf{x}) \oplus g(\mathbf{x})$  on  $\mathbb{F}_2^n$ , then for  $\mathbf{u} \in \mathbb{F}_2^n$ ,

$$\mathcal{H}_h(\mathbf{u}) = 2^{-n/2} \sum_{\mathbf{v} \in \mathbb{F}_2^n} \mathcal{H}_f(\mathbf{v}) \mathcal{W}_g(\mathbf{u} \oplus \mathbf{v}) = 2^{-n/2} \sum_{\mathbf{v} \in \mathbb{F}_2^n} \mathcal{W}_f(\mathbf{v}) \mathcal{H}_g(\mathbf{u} \oplus \mathbf{v}).$$

(iii) If  $h(\mathbf{x}) = f(O\mathbf{x})$ , then  $\mathcal{H}_h(\mathbf{u}) = \zeta^{\text{wt}(\mathbf{a})} \mathcal{H}_f(O\mathbf{u})$ , where  $O$  is an  $n \times n$  orthogonal matrix over  $\mathbb{F}_2$  (and so,  $O^T O = I_n$ ).

(iv) If  $h(\mathbf{x}, \mathbf{y}) = f(\mathbf{x}) \oplus g(\mathbf{y})$ ,  $\mathbf{x}, \mathbf{y} \in \mathbb{F}_2^n$ , then  $\mathcal{H}_{f \oplus g}(\mathbf{u}, \mathbf{v}) = \mathcal{H}_f(\mathbf{u}) \mathcal{H}_g(\mathbf{v})$ .

(v) If  $f \in \mathcal{B}_n, g \in \mathcal{B}_m$ , and  $h(\mathbf{x}, \mathbf{y}) = f(\mathbf{x})g(\mathbf{y})$ , then

$$\begin{aligned} 2^{k/2} \mathcal{H}_h(\mathbf{u}, \mathbf{v}) &= \mathcal{H}_f(\mathbf{u}) A_{g1}(\mathbf{v}) + \omega^n \zeta^{-\text{wt}(\mathbf{u})} A_{g0}(\mathbf{v}), \\ A_{g1}(\mathbf{v}) + A_{g0}(\mathbf{v}) &= (-1)^c 2^m \left( \cos \left( \frac{\pi}{2^k} \right) \right)^m \left( -i \tan \left( \frac{\pi}{2^k} \right) \right)^{\text{wt}(\mathbf{v})} \omega^{m-2\text{wt}(\mathbf{v})}, \end{aligned}$$

where  $A_{g0}(\mathbf{v}) = \sum_{\mathbf{y}, g(\mathbf{y})=0} (-1)^{\mathbf{y} \cdot \mathbf{v}} \zeta^{\text{wt}(\mathbf{v})}$ ,  $A_{g1}(\mathbf{v}) = \sum_{\mathbf{y}, g(\mathbf{y})=1} (-1)^{\mathbf{y} \cdot \mathbf{v}} \zeta^{\text{wt}(\mathbf{v})}$ .  
Moreover, if  $k = 1$ , then  $2^{1/2} \mathcal{H}_{yf(\mathbf{x})}(\mathbf{u}, v) = (-1)^v \zeta \mathcal{H}_f(\mathbf{u}) + 2^{n/2} \left( \cos \left( \frac{\pi}{2^k} \right) \right)^n (-i \tan \left( \frac{\pi}{2^k} \right))^{\text{wt}(\mathbf{u})} \omega^{n-2\text{wt}(\mathbf{u})}$ ,  $2^{1/2} \mathcal{H}_{(y \oplus 1)f(\mathbf{x})}(\mathbf{u}, v) = \mathcal{H}_f(\mathbf{u}) + 2^{n/2} (-1)^v \zeta \left( \cos \left( \frac{\pi}{2^k} \right) \right)^n (-i \tan \left( \frac{\pi}{2^k} \right))^{\text{wt}(\mathbf{u})} \omega^{n-2\text{wt}(\mathbf{u})}$ .

*Proof.* To show (i), write

$$\begin{aligned} \mathcal{H}_{f \oplus \ell_{\mathbf{a}, c}}(\mathbf{u}) &= \sum_{\mathbf{x} \in \mathbb{V}_n} (-1)^{f(\mathbf{x}) \oplus \ell_{\mathbf{a}, c}(\mathbf{x}) \oplus \mathbf{x} \cdot \mathbf{u}} \zeta^{\text{wt}(\mathbf{x})} \\ &= (-1)^c \sum_{\mathbf{x} \in \mathbb{V}_n} (-1)^{f(\mathbf{x}) \oplus \mathbf{x} \cdot (\mathbf{a} \oplus \mathbf{u})} \zeta^{\text{wt}(\mathbf{x})} \\ &= (-1)^c \mathcal{H}_f(\mathbf{a} \oplus \mathbf{u}). \end{aligned}$$

Next, for  $\zeta = e^{\frac{2\pi i}{2^k}}$  and  $\omega = e^{\frac{\pi i}{2^k}}$  a square root of  $\zeta$ , then

$$\begin{aligned} 1 + \zeta &= 1 + \cos \left( \frac{\pi}{2^{k-1}} \right) + i \sin \left( \frac{\pi}{2^{k-1}} \right) \\ &= 2 \cos^2 \left( \frac{\pi}{2^k} \right) + 2i \sin \left( \frac{\pi}{2^k} \right) \cos \left( \frac{\pi}{2^k} \right) \\ &= 2 \cos \left( \frac{\pi}{2^k} \right) e^{\frac{\pi i}{2^k}} = 2 \cos \left( \frac{\pi}{2^k} \right) \omega, \\ 1 - \zeta &= 2 \sin^2 \left( \frac{\pi}{2^k} \right) - 2i \sin \left( \frac{\pi}{2^k} \right) \cos \left( \frac{\pi}{2^k} \right) \\ &= -2i \sin \left( \frac{\pi}{2^k} \right) \omega^{-1}, \end{aligned}$$

so,  $1 + (-1)^b \zeta = \left(2 \cos\left(\frac{\alpha}{2}\right) - \omega \frac{1 - (-1)^b}{2}\right) \omega^{(-1)^b}$ .

Let  $f = 0$ . Then, with notations  $\mathbf{a} = (a_1, \dots, a_n)$ ,  $\mathbf{u} = (u_1, \dots, u_n)$ , and for easy writing,  $b_i := a_i \oplus u_i$ ,  $1 \leq i \leq n$ , we write

$$\begin{aligned}
\mathcal{H}_{\ell_{\mathbf{a}}, c}(\mathbf{u}) &= (-1)^c \sum_{\mathbf{x} \in \mathbb{V}_n} (-1)^{\mathbf{x} \cdot (\mathbf{a} \oplus \mathbf{u})} \zeta^{\text{wt}(\mathbf{x})} \\
&= (-1)^c \prod_{k=1}^n \left(1 + \zeta(-1)^{b_k}\right) \\
&= (-1)^c \prod_{b_k=0} (1 + \zeta) \prod_{b_k=1} (1 - \zeta) \\
&= (-1)^c \left(2 \cos\left(\frac{\pi}{2^k}\right)\right)^{n - \text{wt}(\mathbf{a} \oplus \mathbf{u})} \omega^{n - \text{wt}(\mathbf{a} \oplus \mathbf{u})} \\
&\quad \cdot \left(-2i \sin\left(\frac{\pi}{2^k}\right)\right)^{\text{wt}(\mathbf{a} \oplus \mathbf{u})} \omega^{-\text{wt}(\mathbf{a} \oplus \mathbf{u})} \\
&= (-1)^c 2^n \left(\cos\left(\frac{\pi}{2^k}\right)\right)^n \left(-i \tan\left(\frac{\pi}{2^k}\right)\right)^{\text{wt}(\mathbf{a} \oplus \mathbf{u})} \omega^{n - 2\text{wt}(\mathbf{a} \oplus \mathbf{u})}.
\end{aligned}$$

Next, we show (ii). We write

$$\begin{aligned}
\sum_{\mathbf{v} \in \mathbb{V}_n} \mathcal{H}_f(\mathbf{v}) \mathcal{W}_g(\mathbf{u} \oplus \mathbf{v}) &= 2^{-n} \sum_{\mathbf{v}, \mathbf{y}, \mathbf{z} \in \mathbb{V}_n} (-1)^{f(\mathbf{y}) \oplus g(\mathbf{z}) \oplus \mathbf{v} \cdot (\mathbf{y} \oplus \mathbf{z}) \oplus \mathbf{u} \cdot \mathbf{z}} \zeta^{\text{wt}(\mathbf{y})} \\
&= 2^{-n} \sum_{\mathbf{y}, \mathbf{z} \in \mathbb{V}_n} (-1)^{f(\mathbf{y}) \oplus g(\mathbf{z}) \oplus \mathbf{u} \cdot \mathbf{z}} \zeta^{\text{wt}(\mathbf{y})} \sum_{\mathbf{v} \in \mathbb{V}_n} (-1)^{\mathbf{v} \cdot (\mathbf{y} \oplus \mathbf{z})} \\
&= \sum_{\mathbf{y} \in \mathbb{V}_n} (-1)^{f(\mathbf{y}) \oplus g(\mathbf{y}) \oplus \mathbf{u} \cdot \mathbf{y}} \zeta^{\text{wt}(\mathbf{y})} = 2^{n/2} \mathcal{H}_{f \oplus g}(\mathbf{u}).
\end{aligned}$$

The second identity is similar.

For (iii) we use a similar argument as in [11], and get

$$\begin{aligned}
\mathcal{H}_h(\mathbf{u}) &= 2^{-n/2} \sum_{\mathbf{y}} (-1)^{h(\mathbf{y}) \oplus \mathbf{u} \cdot \mathbf{y}} \zeta^{\text{wt}(\mathbf{y})} = 2^{-n/2} \sum_{\mathbf{y}} (-1)^{f(O\mathbf{y}) \oplus \mathbf{u} \cdot \mathbf{y}} \zeta^{\text{wt}(\mathbf{y})} \\
&= 2^{-n/2} \sum_{\mathbf{z}} (-1)^{f(\mathbf{z}) \oplus \mathbf{u} \cdot O^T \mathbf{z}} \zeta^{\text{wt}(O^T \mathbf{z})} \\
&= 2^{-n/2} \sum_{\mathbf{z}} (-1)^{f(\mathbf{z}) \oplus O\mathbf{u} \cdot \mathbf{z}} \zeta^{\text{wt}(\mathbf{z})} \\
&= 2^{-n/2} \zeta^{\text{wt}(\mathbf{a})} \sum_{\mathbf{z}} (-1)^{f(\mathbf{z}) \oplus (O\mathbf{u}) \cdot \mathbf{z}} \zeta^{\text{wt}(\mathbf{z})} \\
&= \zeta^{\text{wt}(\mathbf{a})} \mathcal{H}_f(O\mathbf{u}),
\end{aligned}$$

since  $\text{wt}(O^T \mathbf{z}) = (O^T \mathbf{z})^T (O^T \mathbf{z}) = \mathbf{z}^T (OO^T) \mathbf{z} = \mathbf{z}^T \mathbf{z} = \text{wt}(\mathbf{z})$ .

Claim (iv) is straightforward, and for claim (v), exactly as in [11] for the nega-Hadamard transform, we see that

$$\begin{aligned}
2^{(n+m)/2} \mathcal{H}_h(\mathbf{u}, \mathbf{v}) &= \sum_{(\mathbf{x}, \mathbf{y}) \in \mathbb{F}_2^{n+k}} (-1)^{f(\mathbf{x})g(\mathbf{y}) \oplus \mathbf{x} \cdot \mathbf{u} \oplus \mathbf{y} \cdot \mathbf{v}} \zeta^{\text{wt}(\mathbf{x}) + \text{wt}(\mathbf{y})} \\
&= \sum_{\mathbf{y}, g(\mathbf{y})=1} (-1)^{\mathbf{y} \cdot \mathbf{v}} \zeta^{\text{wt}(\mathbf{y})} \sum_{\mathbf{x}} (-1)^{f(\mathbf{x}) \oplus \mathbf{x} \cdot \mathbf{u}} \zeta^{\text{wt}(\mathbf{x})} \\
&\quad + \sum_{\mathbf{y}, g(\mathbf{y})=0} (-1)^{\mathbf{y} \cdot \mathbf{v}} \zeta^{\text{wt}(\mathbf{y})} \sum_{\mathbf{x}} (-1)^{\mathbf{x} \cdot \mathbf{u}} \zeta^{\text{wt}(\mathbf{x})} \\
&= 2^{n/2} \mathcal{H}_f(\mathbf{u}) \sum_{\mathbf{y}, g(\mathbf{y})=1} (-1)^{\mathbf{y} \cdot \mathbf{v}} \zeta^{\text{wt}(\mathbf{y})} + 2^n \left( \cos \left( \frac{\pi}{2^k} \right) \right)^n \\
&\quad \cdot \left( -i \tan \left( \frac{\pi}{2^k} \right) \right)^{\text{wt}(\mathbf{u})} \omega^{n-2\text{wt}(\mathbf{u})} \sum_{\mathbf{y}, g(\mathbf{y})=0} (-1)^{\mathbf{y} \cdot \mathbf{v}} \zeta^{\text{wt}(\mathbf{y})},
\end{aligned}$$

from which we obtain the claim. In particular, for  $m = 1$ , if  $g(y) = y$ , then  $A_{g0}(v) = 1$ ,  $A_{g1}(v) = (-1)^v \zeta$ , and if  $g(y) = y \oplus 1$ , then  $A_{g1}(v) = 1$ ,  $A_{g0}(v) = (-1)^v \zeta$ , and so the claim follows.  $\square$

**Theorem 3.** *Let  $f, g \in \mathcal{B}_n$ . The  $2^k$ -crosscorrelation of  $f, g$  is*

$$\mathcal{C}_{f,g}^{(2^k)}(\mathbf{z}) = \zeta^{\text{wt}(\mathbf{z})} \sum_{\mathbf{u} \in \mathbb{V}_n} \mathcal{H}_f(\mathbf{u}) \overline{\mathcal{H}_g(\mathbf{u})} (-1)^{\mathbf{u} \cdot \mathbf{z}}.$$

Furthermore, the  $2^k$ -Parseval identity holds

$$\sum_{\mathbf{u} \in \mathbb{V}_n} |\mathcal{H}_f(\mathbf{u})|^2 = 2^n.$$

Moreover,  $f$  is  $2^k$ -bent if and only if  $\mathcal{C}_f(\mathbf{u}) = 0$ , for all  $\mathbf{u} \neq \mathbf{0}$ .

*Proof.* Using [3, Lemma 2.6] and identity (2), we write

$$\begin{aligned}
&\zeta^{\text{wt}(\mathbf{z})} \sum_{\mathbf{u} \in \mathbb{V}_n} \mathcal{H}_f(\mathbf{u}) \overline{\mathcal{H}_g(\mathbf{u})} (-1)^{\mathbf{u} \cdot \mathbf{z}} \\
&= 2^{-n} \sum_{\mathbf{x}, \mathbf{y} \in \mathbb{V}_n} (-1)^{f(\mathbf{x}) \oplus g(\mathbf{y})} \zeta^{\text{wt}(\mathbf{x}) + \text{wt}(\mathbf{z}) - \text{wt}(\mathbf{y})} \sum_{\mathbf{u} \in \mathbb{V}_n} (-1)^{\mathbf{u} \cdot (\mathbf{x} \oplus \mathbf{y} \oplus \mathbf{z})} \\
&= \sum_{\mathbf{x}, \mathbf{y} \in \mathbb{V}_n} (-1)^{f(\mathbf{x}) \oplus g(\mathbf{x} \oplus \mathbf{z})} \zeta^{2\text{wt}(\mathbf{x} \star \mathbf{z})} \\
&= \sum_{\mathbf{x} \in \mathbb{V}_n} (-1)^{f(\mathbf{x}) \oplus g(\mathbf{x} \oplus \mathbf{z})} \mu^{\mathbf{x} \odot \mathbf{z}} = \mathcal{C}_{f,g}^{(2^k)}(\mathbf{z}).
\end{aligned}$$



If  $f = g$ , then we get

$$\mathcal{C}_f^{(2^k)}(\mathbf{z}) = \sum_{\mathbf{u} \in \mathbb{V}_n} (-1)^{f(\mathbf{u}) \oplus f(\mathbf{u} \oplus \mathbf{z})} \mu^{\mathbf{u} \odot \mathbf{z}} = \zeta^{\text{wt}(\mathbf{z})} \sum_{\mathbf{u} \in \mathbb{V}_n} |\mathcal{H}_f(\mathbf{u})|^2 (-1)^{\mathbf{u} \cdot \mathbf{z}},$$

and by replacing  $z = 0$ , then we get the  $2^k$ -Parseval identity. The last claim is also implied by the previous identity.  $\square$

### 3 Complete characterization of octabent and hexabent Boolean functions

**Lemma 4.** *Let  $z$  be a complex number. If  $s \in \mathbb{Z}_2$ , then*

$$z^s = \frac{1 + (-1)^s}{2} + \frac{1 - (-1)^s}{2} z. \quad (3)$$

*Proof.* The claim is a straightforward computation going through the cases  $s = 0, 1$ .  $\square$

Throughout the paper, we let

$$\begin{aligned} s_1(\mathbf{x}) &= \bigoplus_{i=1}^n x_i, & s_2(\mathbf{x}) &= \bigoplus_{1 \leq i < j \leq n} x_i x_j, \\ s_3(\mathbf{x}) &= \bigoplus_{1 \leq i < j < k \leq n} x_i x_j x_k, & s_4(\mathbf{x}) &= \bigoplus_{1 \leq i < j < k < l \leq n} x_i x_j x_k x_l \\ \text{and, in general,} & & s_t(\mathbf{x}) &= \bigoplus_{1 \leq i_1 < \dots < i_t \leq n} x_{i_1} \cdots x_{i_t}, \end{aligned}$$

be the symmetric polynomials of degree  $1, 2, 3, 4, t$ , etc., respectively, all reduced modulo 2 (we use the convention that  $s_t(\mathbf{x}) = 0$ , if  $\mathbf{x} \in \mathbb{F}_2^\ell$ , and  $\ell < t$ ).

**Lemma 5.** *Let  $\mathbf{x} = (x_1, \dots, x_n) \in \mathbb{V}_n$ . Then*

$$\begin{aligned} \text{wt}(\mathbf{x}) \pmod{8} &= s_1(\mathbf{x}) + 2s_2(\mathbf{x}) + 4s_4(\mathbf{x}) \\ \text{wt}(\mathbf{x}) \pmod{16} &= s_1(\mathbf{x}) + 2s_2(\mathbf{x}) + 4s_4(\mathbf{x}) + 8s_8(\mathbf{x}), \\ \text{wt}(\mathbf{x}) \pmod{2^k} &= \text{wt}(\mathbf{x}) \pmod{2^{k-1}} + 2^{k-1} s_{2^{k-1}}(\mathbf{x}) = \sum_{i=0}^{k-1} 2^i s_{2^i}(\mathbf{x}). \end{aligned}$$

*Proof.* We will be using Newton's identities for symmetric polynomials: with the notations  $\mathbf{x} = (x_1, \dots, x_n)$ ,  $p_i(\mathbf{x}) = \sum_{k=1}^n x_k^i$ ,  $e_0(\mathbf{x}) = 1$ ,  $e_1(\mathbf{x}) = \sum_{k=1}^n x_k$ ,  $e_2(\mathbf{x}) = \sum_{1 \leq k < j \leq n} x_k x_j$ ,  $e_3(\mathbf{x}) = \sum_{1 \leq k < j < s \leq n} x_k x_j x_s$ , etc., then

$$k e_k(\mathbf{x}) = \sum_{i=1}^k (-1)^{i-1} e_{k-i}(\mathbf{x}) p_i(\mathbf{x}).$$

Taking  $k = 3$ , we get  $3e_3 = e_2 p_1 - e_1 p_2 + p_3$ . Reducing this identity modulo 2 and observing that  $p_i(\mathbf{x}) \pmod{2} = s_1(\mathbf{x})$ , for all  $i \geq 1$ , we can write,

$$s_3(\mathbf{x}) = s_2(\mathbf{x}) s_1(\mathbf{x}) \oplus s_1^2(\mathbf{x}) \oplus s_1(\mathbf{x}) = s_2(\mathbf{x}) s_1(\mathbf{x}). \quad (4)$$

In general,

$$s_{2k+1}(\mathbf{x}) = \left( \bigoplus_{i=2}^{2k} s_i(\mathbf{x}) \right) s_1(\mathbf{x}).$$

We show our lemma by induction on  $n$ . The claim is certainly true for  $n = 1, 2$ . Let  $\mathbf{x} = (\mathbf{x}', x_{n+1})$ ,  $\mathbf{x}' \in \mathbb{F}_2^n$ . If  $x_{n+1} = 0$ , then

$$\begin{aligned} \text{wt}(\mathbf{x}) \pmod{8} &= \text{wt}(\mathbf{x}') \pmod{8} \\ &= s_1(\mathbf{x}') + 2s_2(\mathbf{x}') + 4s_4(\mathbf{x}') \pmod{8} \\ &= s_1(\mathbf{x}) + 2s_2(\mathbf{x}) + 4s_4(\mathbf{x}) \pmod{8}. \end{aligned}$$

If  $x_{n+1} = 1$ , then  $s_1(\mathbf{x}) = s_1(\mathbf{x}') \oplus 1$ ,  $s_2(\mathbf{x}) = s_2(\mathbf{x}') \oplus s_1(\mathbf{x}')$ ,  $s_4(\mathbf{x}) = s_4(\mathbf{x}') \oplus s_3(\mathbf{x}') = s_4(\mathbf{x}') \oplus s_1(\mathbf{x}') s_2(\mathbf{x}')$ , using (4). We distinguish several cases.

*Case 1.*  $s_1(\mathbf{x}') = 0$  (thus  $\text{wt}(\mathbf{x}') \pmod{8} < 7$ ). Then

$$\begin{aligned} \text{wt}(\mathbf{x}) \pmod{8} &= \text{wt}(\mathbf{x}') \pmod{8} + 1 \\ &= 1 + s_1(\mathbf{x}') + 2s_2(\mathbf{x}') + 4s_4(\mathbf{x}') \\ &= s_1(\mathbf{x}) + 2s_2(\mathbf{x}) + 4s_4(\mathbf{x}). \end{aligned}$$

*Case 2.*  $s_1(\mathbf{x}') \neq 0$ ,  $s_2(\mathbf{x}') = 0$  (thus  $\text{wt}(\mathbf{x}') \pmod{8} < 7$ ). Then,

$$\begin{aligned} \text{wt}(\mathbf{x}) \pmod{8} &= \text{wt}(\mathbf{x}') \pmod{8} + 1 \\ &= 1 + s_1(\mathbf{x}') + 2s_2(\mathbf{x}') + 4s_4(\mathbf{x}') \\ &= s_1(\mathbf{x}) + 2s_2(\mathbf{x}) + 4s_4(\mathbf{x}), \end{aligned}$$

since  $s_2(\mathbf{x}) = s_1(\mathbf{x}')$  and  $s_1(\mathbf{x}) = 0$ .

Case 3.  $s_1(\mathbf{x}') \neq 0, s_2(\mathbf{x}') \neq 0, s_4(\mathbf{x}') = 0$  (thus  $\text{wt}(\mathbf{x}') \pmod{8} < 7$ ). Then,

$$\begin{aligned}\text{wt}(\mathbf{x}) \pmod{8} &= \text{wt}(\mathbf{x}') \pmod{8} + 1 \\ &= 1 + s_1(\mathbf{x}') + 2s_2(\mathbf{x}') + 4s_4(\mathbf{x}') \\ &= s_1(\mathbf{x}) + 2s_2(\mathbf{x}) + 4s_4(\mathbf{x}),\end{aligned}$$

since  $s_4(\mathbf{x}) = s_1(\mathbf{x}')s_2(\mathbf{x}') = 1$  and  $s_1(\mathbf{x}) = s_2(\mathbf{x}) = 0$ .

Case 4.  $s_1(\mathbf{x}') \neq 0, s_2(\mathbf{x}') \neq 0, s_4(\mathbf{x}') \neq 0$  (thus  $\text{wt}(\mathbf{x}') \pmod{8} = 7$ ). Then,

$$\begin{aligned}0 &= \text{wt}(\mathbf{x}) \pmod{8} \\ &= s_1(\mathbf{x}) + 2s_2(\mathbf{x}) + 4s_4(\mathbf{x}),\end{aligned}$$

since in this case  $s_1(\mathbf{x}) = s_2(\mathbf{x}) = s_4(\mathbf{x}) = 0$ .

The remaining claims can be shown in a similar way, although there are more cases to be considered, however an alternative inductive argument can be used. Let  $\text{wt}(\mathbf{x}) = 2^k t + 2^{k-1} s + p$ , where  $s = 0, 1$  and  $p < 2^{k-1}$ . If  $s = 0$ , then  $\text{wt}(\mathbf{x}) \pmod{2^k} = p = \text{wt}(\mathbf{x}) \pmod{2^{k-1}}$ , so we just need to show that  $s_{2^{k-1}}(\mathbf{x}) = 0$  in this case. Certainly,  $s_{2^{k-1}}(\mathbf{x})$  is exactly the parity of the number of terms in this polynomial, when the variables are taken from the nonzero positions of  $\mathbf{x}$ . That is, we simply need to consider the parity of the binomial coefficient  $\binom{2^k t + p}{2^{k-1}}$ , which is zero by a corollary to a Theorem of Kummer (the binomial coefficient  $\binom{m}{\ell} \equiv 0 \pmod{2}$  if and only if there is a carry when  $\ell$  and  $m - \ell$  are added in base 2, which is equivalent to the statement that  $m$  has no 0 in its binary expansion every time  $\ell$  has a 1). Similarly, if  $s = 1$ , then  $s_{2^{k-1}}(\mathbf{x}) = \binom{2^k t + 2^{k-1} + p}{2^{k-1}} = 1$ , by the same argument. Thus, we get the first equality of the last identity of our lemma, and by induction, the second one is shown, as well.  $\square$

**Theorem 6.** *Let  $f \in \mathcal{B}_n$  and  $\zeta = e^{\frac{2\pi i}{8}}$ . The octa-Hadamard transform of  $f$  can be written as a combination of Walsh-Hadamard transforms in the following way:*

$$4\mathcal{O}_f(\mathbf{u}) = \alpha_1 \mathcal{W}_{f \oplus s_4}(\mathbf{u}) + \alpha_2 \mathcal{W}_{f \oplus s_4}(\bar{\mathbf{u}}) + \alpha_3 \mathcal{W}_{f \oplus s_2 \oplus s_4}(\mathbf{u}) + \alpha_4 \mathcal{W}_{f \oplus s_2 \oplus s_4}(\bar{\mathbf{u}}),$$

where  $\alpha_1 = 1 + \zeta + \zeta^2 + \zeta^3$ ,  $\alpha_2 = 1 - \zeta + \zeta^2 - \zeta^3$ ,  $\alpha_3 = 1 + \zeta - \zeta^2 - \zeta^3$ ,  $\alpha_4 = 1 - \zeta - \zeta^2 + \zeta^3$ . Furthermore,  $f$  is octabent if and only if: for  $n$  even,  $f \oplus s_4$  is bent-negabent (that is, both  $f \oplus s_4$ ,  $f \oplus s_2 \oplus s_4$  are bent) and  $\mathcal{W}_{f \oplus s_4}(\mathbf{u})\mathcal{W}_{f \oplus s_2 \oplus s_4}(\mathbf{u}) = \mathcal{W}_{f \oplus s_4}(\bar{\mathbf{u}})\mathcal{W}_{f \oplus s_2 \oplus s_4}(\bar{\mathbf{u}})$ ; for  $n$  odd,  $f \oplus s_2, f \oplus s_2 \oplus s_4$  are both semibent such that  $|\mathcal{W}_{f \oplus s_4}(\mathbf{u})| = |\mathcal{W}_{f \oplus s_4}(\bar{\mathbf{u}})| = \sqrt{2}$ ,  $\mathcal{W}_{f \oplus s_2 \oplus s_4}(\mathbf{u}) = \mathcal{W}_{f \oplus s_2 \oplus s_4}(\bar{\mathbf{u}}) = 0$ , or  $\mathcal{W}_{f \oplus s_4}(\mathbf{u}) = \mathcal{W}_{f \oplus s_4}(\bar{\mathbf{u}}) = 0$ ,  $|\mathcal{W}_{f \oplus s_2 \oplus s_4}(\mathbf{u})| = |\mathcal{W}_{f \oplus s_2 \oplus s_4}(\bar{\mathbf{u}})| = \sqrt{2}$ .

*Proof.* Using Lemmas 4 and 5, we write (recall that in this case  $\zeta = e^{\frac{2\pi i}{8}}$ )

$$\begin{aligned}
4\mathcal{O}_f(\mathbf{u}) &= 2^{-\frac{n}{2}+2} \sum_{\mathbf{x} \in \mathbb{V}_n} (-1)^{f(\mathbf{x}) \oplus \mathbf{u} \cdot \mathbf{x}} \zeta^{\text{wt}(\mathbf{x})} \\
&= 2^{-\frac{n}{2}+2} \sum_{\mathbf{x} \in \mathbb{V}_n} (-1)^{f(\mathbf{x}) \oplus \mathbf{u} \cdot \mathbf{x}} \zeta^{s_1(\mathbf{x})+2s_2(\mathbf{x})+4s_4(\mathbf{x})} \\
&= 2^{-\frac{n}{2}+2} \sum_{\mathbf{x} \in \mathbb{V}_n} (-1)^{f(\mathbf{x}) \oplus \mathbf{u} \cdot \mathbf{x}} \zeta^{s_1(\mathbf{x})} i^{s_2(\mathbf{x})} (-1)^{s_4(\mathbf{x})} \\
&= 2^{-\frac{n}{2}+2} \sum_{\mathbf{x} \in \mathbb{V}_n} (-1)^{f(\mathbf{x}) \oplus s_4(\mathbf{x}) + \mathbf{u} \cdot \mathbf{x}} \left( (1 + (-1)^{s_1(\mathbf{x})}) + (1 - (-1)^{s_1(\mathbf{x})}) \zeta \right) \\
&\quad \cdot \left( (1 + (-1)^{s_2(\mathbf{x})}) + (1 - (-1)^{s_2(\mathbf{x})}) i \right) \\
&= \alpha_1 2^{-\frac{n}{2}} \sum_{\mathbf{x} \in \mathbb{V}_n} (-1)^{f(\mathbf{x}) \oplus s_4(\mathbf{x}) \oplus \mathbf{u} \cdot \mathbf{x}} \\
&\quad + \alpha_2 2^{-\frac{n}{2}} \sum_{\mathbf{x} \in \mathbb{V}_n} (-1)^{f(\mathbf{x}) \oplus s_1(\mathbf{x}) \oplus s_4(\mathbf{x}) \oplus \mathbf{u} \cdot \mathbf{x}} \\
&\quad + \alpha_3 2^{-\frac{n}{2}} \sum_{\mathbf{x} \in \mathbb{V}_n} (-1)^{f(\mathbf{x}) \oplus s_2(\mathbf{x}) \oplus s_4(\mathbf{x}) \oplus \mathbf{u} \cdot \mathbf{x}} \\
&\quad + \alpha_4 2^{-\frac{n}{2}} \sum_{\mathbf{x} \in \mathbb{V}_n} (-1)^{f(\mathbf{x}) \oplus s_1(\mathbf{x}) \oplus s_2(\mathbf{x}) \oplus s_4(\mathbf{x}) \oplus \mathbf{u} \cdot \mathbf{x}} \\
&= \alpha_1 \mathcal{W}_{f \oplus s_4}(\mathbf{u}) + \alpha_2 \mathcal{W}_{f \oplus s_1 \oplus s_4}(\mathbf{u}) + \alpha_3 \mathcal{W}_{f \oplus s_2 \oplus s_4}(\mathbf{u}) + \alpha_4 \mathcal{W}_{f \oplus s_1 \oplus s_2 \oplus s_4}(\mathbf{u}) \\
&= \alpha_1 \mathcal{W}_{f \oplus s_4}(\mathbf{u}) + \alpha_2 \mathcal{W}_{f \oplus s_4}(\bar{\mathbf{u}}) + \alpha_3 \mathcal{W}_{f \oplus s_2 \oplus s_4}(\mathbf{u}) + \alpha_4 \mathcal{W}_{f \oplus s_2 \oplus s_4}(\bar{\mathbf{u}}),
\end{aligned}$$

where  $\alpha_1 = 1 + \zeta + \zeta^2 + \zeta^3$ ,  $\alpha_2 = 1 - \zeta + \zeta^2 - \zeta^3$ ,  $\alpha_3 = 1 + \zeta - \zeta^2 - \zeta^3$ ,  $\alpha_4 = 1 - \zeta - \zeta^2 + \zeta^3$ .

Denoting  $X = \mathcal{W}_{f \oplus s_4}(\mathbf{u})$ ,  $Y = \mathcal{W}_{f \oplus s_1 \oplus s_4}(\mathbf{u}) = \mathcal{W}_{f \oplus s_4}(\bar{\mathbf{u}})$ ,  $W = \mathcal{W}_{f \oplus s_2 \oplus s_4}(\mathbf{u})$ ,  $Z = \mathcal{W}_{f \oplus s_1 \oplus s_2 \oplus s_4}(\mathbf{u}) = \mathcal{W}_{f \oplus s_2 \oplus s_4}(\bar{\mathbf{u}})$ , we further obtain

$$\begin{aligned}
4\mathcal{O}_f(\mathbf{u}) &= (W + X + Y + Z) + \sqrt{2}(W - Z) \\
&\quad + i(X + Y - W - Z) + i\sqrt{2}(X - Y),
\end{aligned}$$

and therefore,

$$16|\mathcal{O}_f(\mathbf{u})|^2 = 4(X^2 + Y^2 + W^2 + Z^2) + 2\sqrt{2}(X^2 + W^2 - Y^2 - Z^2 + 2WY - 2XZ).$$

If  $f$  is octabent, that is,  $|\mathcal{O}_f(\mathbf{u})| = 1$ , for all  $\mathbf{u}$ , then, we obtain the following system of equations

$$\begin{aligned}
X^2 + Y^2 + W^2 + Z^2 &= 4 \\
X^2 + W^2 - Y^2 - Z^2 + 2WY - 2XZ &= 0.
\end{aligned}$$

If  $n$  is even, then by Jacobi's four-squares theorem, we obtain the solutions  $(X, Y, W, Z)$

$$\begin{aligned} &(-1, -1, -1, -1), (-1, -1, 1, 1), (-1, 1, -1, 1), (-1, 1, 1, -1), \\ &(1, -1, -1, 1), (1, -1, 1, -1), (1, 1, -1, -1), (1, 1, 1, 1). \end{aligned}$$

Thus,  $f \oplus s_4, f \oplus s_2 \oplus s_4$  are both bent such that  $\mathcal{W}_{f \oplus s_4}(\mathbf{u})\mathcal{W}_{f \oplus s_2 \oplus s_4}(\mathbf{u}) = \mathcal{W}_{f \oplus s_4}(\bar{\mathbf{u}})\mathcal{W}_{f \oplus s_2 \oplus s_4}(\bar{\mathbf{u}})$ . If  $n$  is odd, then the same system will have solutions  $(X, Y, W, Z)$

$$\begin{aligned} &(-\sqrt{2}, -\sqrt{2}, 0, 0), (-\sqrt{2}, \sqrt{2}, 0, 0), (0, 0, -\sqrt{2}, -\sqrt{2}), (0, 0, -\sqrt{2}, \sqrt{2}), \\ &(0, 0, \sqrt{2}, -\sqrt{2}), (0, 0, \sqrt{2}, \sqrt{2}), (\sqrt{2}, -\sqrt{2}, 0, 0), (\sqrt{2}, \sqrt{2}, 0, 0). \end{aligned}$$

$|\mathcal{W}_{f \oplus s_4}(\mathbf{u})| = |\mathcal{W}_{f \oplus s_4}(\bar{\mathbf{u}})| = 1$  and  $\mathcal{W}_{f \oplus s_2 \oplus s_4}(\mathbf{u}) = \mathcal{W}_{f \oplus s_2 \oplus s_4}(\bar{\mathbf{u}}) = 0$ , or  $\mathcal{W}_{f \oplus s_4}(\mathbf{u}) = \mathcal{W}_{f \oplus s_4}(\bar{\mathbf{u}}) = 0$  and  $|\mathcal{W}_{f \oplus s_2 \oplus s_4}(\mathbf{u})| = |\mathcal{W}_{f \oplus s_2 \oplus s_4}(\bar{\mathbf{u}})| = 1$ .

A simple computation shows that for these values,  $f$  is octabent, and the theorem is shown.  $\square$

**Remark 7.** *Given our definition, we see that  $f$  is octabent if and only if  $f \oplus s_4$  is a strong negabent function, together with some conditions on the Walsh coefficients.*

**Corollary 8.** *If  $f$  is octabent,  $\zeta = e^{\frac{2\pi}{8}}$ , then the octa-Hadamard spectrum of  $f$  is  $\{\zeta^k \mid 0 \leq k \leq 8\} = \{\pm 1, \pm \zeta, \pm i, \pm \zeta^3\}$ . If  $f$  is a weak octabent, then its spectrum in absolute value belongs to  $\{1, \sqrt{1 \pm \frac{1}{\sqrt{2}}}\}$ .*

*Proof.* The proof is a straightforward computation running through the set of values for the Walsh-Hadamard coefficients described in the previous theorem, respectively, all  $\pm 1$  coefficients for the second claim.  $\square$

**Corollary 9.** *Let  $n$  be odd and  $f \in \mathcal{B}_n$ . Then  $f$  is octabent if and only if  $g_1(\mathbf{x}, y) = f(\mathbf{x}) \oplus s_4(\mathbf{x}) \oplus y s_2(\mathbf{x})$ ,  $g_2(\mathbf{x}, y) = f(\mathbf{x}) \oplus s_4(\mathbf{x}) \oplus y(s_2(\mathbf{x}) \oplus s_1(\mathbf{x}))$  and  $g_3(\mathbf{x}, y) = f(\mathbf{x}) \oplus s_4(\mathbf{x}) \oplus s_1(\mathbf{x}) \oplus y s_2(\mathbf{x})$  are all bent in  $\mathcal{B}_{n+1}$ .*

*Proof.* We compute the Walsh-Hadamard transform of  $g_1$  by

$$\begin{aligned}
\mathcal{W}_{g_1}(\mathbf{u}, v) &= 2^{-\frac{n+1}{2}} \sum_{\substack{\mathbf{x} \in \mathbb{V}_n \\ y \in \mathbb{F}_2}} (-1)^{f(\mathbf{x}) \oplus s_4(\mathbf{x}) \oplus y s_2(\mathbf{x}) \oplus \mathbf{u} \cdot \mathbf{x} \oplus y v} \\
&= 2^{-\frac{n+1}{2}} \sum_{\mathbf{x} \in \mathbb{V}_n} (-1)^{f(\mathbf{x}) \oplus s_4(\mathbf{x}) \oplus \mathbf{u} \cdot \mathbf{x}} \\
&\quad + 2^{-\frac{n+1}{2}} \sum_{\mathbf{x} \in \mathbb{V}_n} (-1)^{f(\mathbf{x}) \oplus s_4(\mathbf{x}) \oplus s_2(\mathbf{x}) \oplus \mathbf{u} \cdot \mathbf{x} \oplus v} \\
&= \frac{1}{\sqrt{2}} (\mathcal{W}_{f \oplus s_4}(\mathbf{u}) + (-1)^v \mathcal{W}_{f \oplus s_2 \oplus s_4}(\mathbf{u})).
\end{aligned}$$

Similarly,

$$\begin{aligned}
\mathcal{W}_{g_2}(\mathbf{u}, v) &= \frac{1}{\sqrt{2}} (\mathcal{W}_{f \oplus s_4}(\mathbf{u}) + (-1)^v \mathcal{W}_{f \oplus s_4 \oplus s_2}(\bar{\mathbf{u}})) \\
\mathcal{W}_{g_3}(\mathbf{u}, v) &= \frac{1}{\sqrt{2}} (\mathcal{W}_{f \oplus s_4}(\bar{\mathbf{u}}) + (-1)^v \mathcal{W}_{f \oplus s_4 \oplus s_2}(\mathbf{u})).
\end{aligned}$$

If  $g_1, g_2, g_3$  are bent, then  $\mathcal{W}_{g_1}(\mathbf{u}, v), \mathcal{W}_{g_2}(\mathbf{u}, v), \mathcal{W}_{g_3}(\mathbf{u}, v) \in \{\pm 1\}$  which implies (by solving the corresponding systems for every possible  $\pm 1$  value) that the Walsh coefficients of  $f \oplus s_2, f \oplus s_2 \oplus s_4$ , etc., are all in  $\{0, \pm\sqrt{2}\}$  and so, these functions are semibent. If,  $|\mathcal{W}_{f \oplus s_4}(\mathbf{u})| = \sqrt{2}$ , then  $\mathcal{W}_{f \oplus s_2 \oplus s_4}(\mathbf{u}) = 0$ , and so (using  $\mathcal{W}_{g_2}$ ),  $|\mathcal{W}_{f \oplus s_2 \oplus s_4}(\bar{\mathbf{u}})| = 0$ , which forces  $|\mathcal{W}_{f \oplus s_4}(\bar{\mathbf{u}})| = \sqrt{2}$ . A similar argument works if  $\mathcal{W}_{f \oplus s_4}(\mathbf{u}) = 0$ . By Theorem 6, then  $f$  is octabent.

Conversely, if  $f$  is octabent, then  $f \oplus s_2, f \oplus s_2 \oplus s_4$  are semibent and either  $|\mathcal{W}_{f \oplus s_4}(\mathbf{u})| = \sqrt{2}$  and  $\mathcal{W}_{f \oplus s_4 \oplus s_2}(\mathbf{u}) = 0$ , or  $\mathcal{W}_{f \oplus s_4}(\mathbf{u}) = 0$  and  $|\mathcal{W}_{f \oplus s_4 \oplus s_2}(\mathbf{u})| = \sqrt{2}$  and thus,  $|\mathcal{W}_{f \oplus s_4}(\mathbf{u}) \pm \mathcal{W}_{f \oplus s_2 \oplus s_4}(\mathbf{u})| = \sqrt{2}$ ,  $|\mathcal{W}_{f \oplus s_4}(\mathbf{u}) \pm \mathcal{W}_{f \oplus s_4 \oplus s_2}(\bar{\mathbf{u}})| = \sqrt{2}$  and  $|\mathcal{W}_{f \oplus s_4}(\bar{\mathbf{u}}) \pm \mathcal{W}_{f \oplus s_4 \oplus s_2}(\mathbf{u})| = \sqrt{2}$ , that is,  $g_1, g_2, g_3$  are all bent.  $\square$

It is known that (when  $n$  is even)  $f$  is negabent if and only if  $f \oplus s_2$  is bent. Thus our condition in the theorem can be rewritten (when  $n$  is even) as  $f$  is octabent if and only if  $f \oplus s_4$  is both bent-negabent (along with the constraint on the spectra). From previous work [7], we know that  $x_1 x_2 \oplus x_2 x_3 \oplus x_3 x_4$  is both bent-negabent. This quickly gives us our first example of weak octabent function, namely  $f(x_1, x_2, x_3, x_4) = x_1 x_2 \oplus x_2 x_3 \oplus x_3 x_4 \oplus x_1 x_2 x_3 x_4$ . In reality, it is not difficult to give examples of weak octabent functions. Let  $\pi$  be a permutation on  $\mathbb{F}_2^n$  such that  $\pi(\mathbf{y}) \oplus \mathbf{y}$  is also a permutation (see the discussion on complete mapping polynomials from [4, 11, 12]). On  $\mathbb{F}_2^{2n}$ , let the Maiorana-McFarland type function  $f(\mathbf{x}, \mathbf{y}) = \mathbf{x} \cdot \pi(\mathbf{y}) \oplus g(\mathbf{y})$ , for some  $g$ ,

and  $f'(\mathbf{x}, \mathbf{y}) = f((\mathbf{x}, \mathbf{y}) \cdot O \oplus \alpha) + \mathbf{a} \cdot \mathbf{x} \oplus c$ , where  $O$  is an orthogonal matrix. We know that  $f'$  is bent-negabent and therefore  $f' \oplus s_4$  is a weak octabent. However, it is not that straightforward to construct (full)  $2^k$ -bent functions.

Next, we characterize hexabent functions.

**Theorem 10.** *Let  $f \in \mathcal{B}_n$  and  $\zeta = e^{\frac{2\pi i}{16}}$ . The hexa-Hadamard transform of  $f$  can be written as a combination of Walsh-Hadamard transforms in the following way:*

$$\begin{aligned} 8\mathcal{X}_f(\mathbf{u}) = & \beta_1 \mathcal{W}_{f \oplus s_8}(\mathbf{u}) + \beta_2 \mathcal{W}_{f \oplus s_8}(\bar{\mathbf{u}}) + \beta_3 \mathcal{W}_{f \oplus s_2 \oplus s_8}(\mathbf{u}) + \beta_4 \mathcal{W}_{f \oplus s_2 \oplus s_8}(\bar{\mathbf{u}}) \\ & + \beta_5 \mathcal{W}_{f \oplus s_4 \oplus s_8}(\mathbf{u}) + \beta_6 \mathcal{W}_{f \oplus s_4 \oplus s_8}(\bar{\mathbf{u}}) \\ & + \beta_7 \mathcal{W}_{f \oplus s_2 \oplus s_4 \oplus s_8}(\mathbf{u}) + \beta_8 \mathcal{W}_{f \oplus s_2 \oplus s_4 \oplus s_8}(\bar{\mathbf{u}}), \end{aligned}$$

where  $\beta_1 = 1 + \zeta + \zeta^2 + \zeta^3 + \zeta^4 + \zeta^5 + \zeta^6 + \zeta^7$ ,  $\beta_2 = 1 - \zeta + \zeta^2 - \zeta^3 + \zeta^4 - \zeta^5 + \zeta^6 - \zeta^7$ ,  $\beta_3 = 1 + \zeta - \zeta^2 - \zeta^3 + \zeta^4 + \zeta^5 - \zeta^6 - \zeta^7$ ,  $\beta_4 = 1 - \zeta - \zeta^2 + \zeta^3 + \zeta^4 - \zeta^5 - \zeta^6 + \zeta^7$ ,  $\beta_5 = 1 + \zeta + \zeta^2 + \zeta^3 - \zeta^4 - \zeta^5 - \zeta^6 - \zeta^7$ ,  $\beta_6 = 1 - \zeta + \zeta^2 - \zeta^3 - \zeta^4 + \zeta^5 - \zeta^6 + \zeta^7$ ,  $\beta_7 = 1 + \zeta - \zeta^2 - \zeta^3 - \zeta^4 - \zeta^5 + \zeta^6 + \zeta^7$ ,  $\beta_8 = 1 - \zeta - \zeta^2 + \zeta^3 - \zeta^4 + \zeta^5 + \zeta^6 - \zeta^7$ . Furthermore,  $f$  is hexabent if and only if conditions (i), for  $n$  even, respectively, (ii), for  $n$  odd hold:

1.  $f \oplus s_8$  is bent-negabent-octabent with the conditions that  $(W_{f \oplus s_8}(\mathbf{u}), W_{f \oplus s_8}(\bar{\mathbf{u}}), W_{f \oplus s_2 \oplus s_8}(\mathbf{u}), W_{f \oplus s_2 \oplus s_8}(\bar{\mathbf{u}}), W_{f \oplus s_4 \oplus s_8}(\mathbf{u}), W_{f \oplus s_4 \oplus s_8}(\bar{\mathbf{u}}), W_{f \oplus s_2 \oplus s_4 \oplus s_8}(\mathbf{u}), W_{f \oplus s_2 \oplus s_4 \oplus s_8}(\bar{\mathbf{u}})) = (1, 1, 1, 1, 1, 1, 1, 1) \star (-1)^\ell$ , where  $\ell \in \mathcal{A}_3$ , and  $\mathcal{A}_3$  is the set of affine functions in three variables.
2.  $f \oplus s_8, f \oplus s_2 \oplus s_8, f \oplus s_4 \oplus s_8, f \oplus s_2 \oplus s_4 \oplus s_8$  are all semibent and  $(W_{f \oplus s_8}(\mathbf{u}), W_{f \oplus s_8}(\bar{\mathbf{u}}), W_{f \oplus s_2 \oplus s_8}(\mathbf{u}), W_{f \oplus s_2 \oplus s_8}(\bar{\mathbf{u}})) = (\sqrt{2}, \sqrt{2}, \sqrt{2}, \sqrt{2}) \star (-1)^\ell$ ,  $\ell \in \mathcal{A}_2$ , and  $\mathcal{A}_2$  is the set of affine functions in two variables, and  $W_{f \oplus s_4 \oplus s_8}(\mathbf{u}) = W_{f \oplus s_4 \oplus s_8}(\bar{\mathbf{u}}) = W_{f \oplus s_2 \oplus s_4 \oplus s_8}(\mathbf{u}) = W_{f \oplus s_2 \oplus s_4 \oplus s_8}(\bar{\mathbf{u}}) = 0$ ; or,  $(W_{f \oplus s_4 \oplus s_8}(\mathbf{u}), W_{f \oplus s_4 \oplus s_8}(\bar{\mathbf{u}}), W_{f \oplus s_2 \oplus s_4 \oplus s_8}(\mathbf{u}), W_{f \oplus s_2 \oplus s_4 \oplus s_8}(\bar{\mathbf{u}})) = (\sqrt{2}, \sqrt{2}, \sqrt{2}, \sqrt{2}) \star (-1)^\ell$ ,  $\ell \in \mathcal{A}_2$ , and  $W_{f \oplus s_8}(\mathbf{u}) = W_{f \oplus s_8}(\bar{\mathbf{u}}) = W_{f \oplus s_2 \oplus s_8}(\mathbf{u}) = W_{f \oplus s_2 \oplus s_8}(\bar{\mathbf{u}}) = 0$ .

*Proof.* As in the previous theorem, we write (here, we set  $\zeta := \zeta_{16} = e^{\frac{2\pi i}{16}}$ )

$$\begin{aligned} 8\mathcal{X}_f(\mathbf{u}) &= 2^{-\frac{n}{2}+3} \sum_{\mathbf{x} \in \mathbb{V}_n} (-1)^{f(\mathbf{x}) \oplus \mathbf{u} \cdot \mathbf{x}} \zeta^{\text{wt}(\mathbf{x})} \\ &= 2^{-\frac{n}{2}+3} \sum_{\mathbf{x} \in \mathbb{V}_n} (-1)^{f(\mathbf{x}) \oplus \mathbf{u} \cdot \mathbf{x}} \zeta^{s_1(\mathbf{x}) + 2s_2(\mathbf{x}) + 4s_4(\mathbf{x}) + 8s_8(\mathbf{x})} \\ &= 2^{-\frac{n}{2}+3} \sum_{\mathbf{x} \in \mathbb{V}_n} (-1)^{f(\mathbf{x}) \oplus \mathbf{u} \cdot \mathbf{x}} \zeta^{s_1(\mathbf{x})} \zeta^{s_2(\mathbf{x})} \zeta^{s_4(\mathbf{x})} (-1)^{s_8(\mathbf{x})} \end{aligned}$$

$$\begin{aligned}
&= 2^{-\frac{n}{2}+3} \sum_{\mathbf{x} \in \mathbb{V}_n} (-1)^{f(\mathbf{x}) \oplus s_8(\mathbf{x}) \oplus \mathbf{u} \cdot \mathbf{x}} \left( (1 + (-1)^{s_1(\mathbf{x})}) + (1 - (-1)^{s_1(\mathbf{x})}) \zeta \right) \\
&\quad \cdot \left( (1 + (-1)^{s_2(\mathbf{x})}) + (1 - (-1)^{s_2(\mathbf{x})}) \zeta_8 \right) \\
&\quad \cdot \left( (1 + (-1)^{s_4(\mathbf{x})}) + (1 - (-1)^{s_4(\mathbf{x})}) i \right) \\
&= \beta_1 2^{-\frac{n}{2}} \sum_{\mathbf{x} \in \mathbb{V}_n} (-1)^{f(\mathbf{x}) \oplus s_8(\mathbf{x}) \oplus \mathbf{u} \cdot \mathbf{x}} \\
&\quad + \beta_2 2^{-\frac{n}{2}} \sum_{\mathbf{x} \in \mathbb{V}_n} (-1)^{f(\mathbf{x}) \oplus s_1(\mathbf{x}) \oplus s_8(\mathbf{x}) \oplus \mathbf{u} \cdot \mathbf{x}} \\
&\quad + \beta_3 2^{-\frac{n}{2}} \sum_{\mathbf{x} \in \mathbb{V}_n} (-1)^{f(\mathbf{x}) \oplus s_2(\mathbf{x}) \oplus s_8(\mathbf{x}) \oplus \mathbf{u} \cdot \mathbf{x}} \\
&\quad + \beta_4 2^{-\frac{n}{2}} \sum_{\mathbf{x} \in \mathbb{V}_n} (-1)^{f(\mathbf{x}) \oplus s_1(\mathbf{x}) \oplus s_2(\mathbf{x}) \oplus s_8(\mathbf{x}) \oplus \mathbf{u} \cdot \mathbf{x}} \\
&\quad + \beta_5 2^{-\frac{n}{2}} \sum_{\mathbf{x} \in \mathbb{V}_n} (-1)^{f(\mathbf{x}) \oplus s_4(\mathbf{x}) \oplus s_8(\mathbf{x}) \oplus \mathbf{u} \cdot \mathbf{x}} \\
&\quad + \beta_6 2^{-\frac{n}{2}} \sum_{\mathbf{x} \in \mathbb{V}_n} (-1)^{f(\mathbf{x}) \oplus s_1(\mathbf{x}) \oplus s_4(\mathbf{x}) \oplus s_8(\mathbf{x}) \oplus \mathbf{u} \cdot \mathbf{x}} \\
&\quad + \beta_7 2^{-\frac{n}{2}} \sum_{\mathbf{x} \in \mathbb{V}_n} (-1)^{f(\mathbf{x}) \oplus s_2(\mathbf{x}) \oplus s_4(\mathbf{x}) \oplus s_8(\mathbf{x}) \oplus \mathbf{u} \cdot \mathbf{x}} \\
&\quad + \beta_8 2^{-\frac{n}{2}} \sum_{\mathbf{x} \in \mathbb{V}_n} (-1)^{f(\mathbf{x}) \oplus s_1(\mathbf{x}) \oplus s_2(\mathbf{x}) \oplus s_4(\mathbf{x}) \oplus s_8(\mathbf{x}) \oplus \mathbf{u} \cdot \mathbf{x}} \\
&= \beta_1 \mathcal{W}_{f \oplus s_8}(\mathbf{u}) + \beta_2 \mathcal{W}_{f \oplus s_8}(\bar{\mathbf{u}}) + \beta_3 \mathcal{W}_{f \oplus s_2 \oplus s_8}(\mathbf{u}) + \beta_4 \mathcal{W}_{f \oplus s_2 \oplus s_8}(\bar{\mathbf{u}}) \\
&\quad + \beta_5 \mathcal{W}_{f \oplus s_4 \oplus s_8}(\mathbf{u}) + \beta_6 \mathcal{W}_{f \oplus s_4 \oplus s_8}(\bar{\mathbf{u}}) + \beta_7 \mathcal{W}_{f \oplus s_2 \oplus s_4 \oplus s_8}(\mathbf{u}) + \beta_8 \mathcal{W}_{f \oplus s_2 \oplus s_4 \oplus s_8}(\bar{\mathbf{u}}),
\end{aligned}$$

$$\begin{aligned}
&\text{where } \beta_1 = 1 + \zeta + \zeta^2 + \zeta^3 + \zeta^4 + \zeta^5 + \zeta^6 + \zeta^7 = 1 + i \left( 1 + \sqrt{2} + \sqrt{2(2 + \sqrt{2})} \right), \\
&\beta_2 = 1 - \zeta + \zeta^2 - \zeta^3 + \zeta^4 - \zeta^5 + \zeta^6 - \zeta^7 = 1 + i \left( 1 + \sqrt{2} - \sqrt{2(2 + \sqrt{2})} \right), \\
&\beta_3 = 1 + \zeta - \zeta^2 - \zeta^3 + \zeta^4 + \zeta^5 - \zeta^6 - \zeta^7 = 1 + \sqrt{4 - 2\sqrt{2}} + i(1 - \sqrt{2}), \\
&\beta_4 = 1 - \zeta - \zeta^2 + \zeta^3 + \zeta^4 - \zeta^5 - \zeta^6 + \zeta^7 = 1 - \sqrt{4 - 2\sqrt{2}} + i(1 - \sqrt{2}), \\
&\beta_5 = 1 + \zeta + \zeta^2 + \zeta^3 - \zeta^4 - \zeta^5 - \zeta^6 - \zeta^7 = (1 - i) + \sqrt{2} + \sqrt{2(2 + \sqrt{2})}, \\
&\beta_6 = 1 - \zeta + \zeta^2 - \zeta^3 - \zeta^4 + \zeta^5 - \zeta^6 + \zeta^7 = (1 - i) + \sqrt{2} - \sqrt{2(2 + \sqrt{2})}, \\
&\beta_7 = 1 + \zeta - \zeta^2 - \zeta^3 - \zeta^4 - \zeta^5 + \zeta^6 + \zeta^7 = 1 - \sqrt{2} + i(-1 - \sqrt{4 - 2\sqrt{2}}), \\
&\beta_8 = 1 - \zeta - \zeta^2 + \zeta^3 - \zeta^4 + \zeta^5 + \zeta^6 - \zeta^7 = 1 - \sqrt{2} + i(\sqrt{4 - 2\sqrt{2}} - 1).
\end{aligned}$$

$$\begin{aligned}
&\text{Set } A := \mathcal{W}_{f \oplus s_8}(\mathbf{u}), B := \mathcal{W}_{f \oplus s_8}(\bar{\mathbf{u}}), C := \mathcal{W}_{f \oplus s_2 \oplus s_8}(\mathbf{u}), D := \mathcal{W}_{f \oplus s_2 \oplus s_8}(\bar{\mathbf{u}}), \\
&X := \mathcal{W}_{f \oplus s_4 \oplus s_8}(\mathbf{u}), Y := \mathcal{W}_{f \oplus s_4 \oplus s_8}(\bar{\mathbf{u}}), W := \mathcal{W}_{f \oplus s_2 \oplus s_4 \oplus s_8}(\mathbf{u}), Z := \mathcal{W}_{f \oplus s_2 \oplus s_4 \oplus s_8}(\bar{\mathbf{u}}).
\end{aligned}$$



Taking the complex norm and arranging the coefficients (as in [6]), we get

$$\begin{aligned}
64|\mathcal{X}_f(\mathbf{u})|^2 = & 8(A^2 + B^2 + C^2 + D^2 + W^2 + X^2 + Y^2 + Z^2) \\
& + 4\sqrt{2}(A^2 + B^2 - C^2 - D^2 - 2AW - W^2 + 2CX + X^2 + 2DY \\
& \quad + Y^2 - 2BZ - Z^2) \\
& + 4\sqrt{4 + 2\sqrt{2}}(A^2 - B^2 - AW + DW + BX + CX + X^2 - AY - DY \\
& \quad - Y^2 + BZ - CZ) \\
& + 2\sqrt{4 - 2\sqrt{2}}(A^2 - B^2 + 2BC + C^2 - 2AD - D^2 - 4DW + W^2 + X^2 \\
& \quad + 2WY - Y^2 + 4CZ - 2XZ - Z^2).
\end{aligned}$$

We now assume that  $f$  is hexabent, so  $|\mathcal{X}_f(\mathbf{u})| = 1$ , for all  $\mathbf{u} \in \mathbb{V}_n$ . We obtain the following system of equations with solutions in  $2^{-n/2}\mathbb{Z}$ ,

$$\begin{aligned}
A^2 + B^2 + C^2 + D^2 + W^2 + X^2 + Y^2 + Z^2 &= 8 \\
A^2 + B^2 - C^2 - D^2 - 2AW - W^2 + 2CX + X^2 + 2DY + Y^2 - 2BZ - Z^2 &= 0 \\
A^2 - B^2 - AW + DW + BX + CX + X^2 - AY - DY - Y^2 + BZ - CZ &= 0 \\
A^2 - B^2 + 2BC + C^2 - 2AD - D^2 - 4DW + W^2 + X^2 \\
&+ 2WY - Y^2 + 4CZ - 2XZ - Z^2 = 0.
\end{aligned}$$

By a similar method as in [6], we can show that if  $n$  is even, then the above system has the solutions

$$\begin{aligned}
& (-1, -1, -1, -1, -1, -1, -1, -1), (-1, -1, -1, -1, 1, 1, 1, 1), \\
& (-1, -1, 1, 1, -1, -1, 1, 1), (-1, -1, 1, 1, 1, 1, -1, -1), \\
& (-1, 1, -1, 1, -1, 1, -1, 1), (-1, 1, -1, 1, 1, -1, 1, -1), \\
& (-1, 1, 1, -1, -1, 1, 1, -1), (-1, 1, 1, -1, 1, -1, -1, 1), \\
& (1, -1, -1, 1, -1, 1, 1, -1), (1, -1, -1, 1, 1, -1, -1, 1), \\
& (1, -1, 1, -1, -1, 1, -1, 1), (1, -1, 1, -1, 1, -1, 1, -1), \\
& (1, 1, -1, -1, -1, -1, 1, 1), (1, 1, -1, -1, 1, 1, -1, -1), \\
& (1, 1, 1, 1, -1, -1, -1, -1), (1, 1, 1, 1, 1, 1, 1, 1).
\end{aligned}$$

Similarly, if  $n$  is odd, the system has the solutions

$$\begin{aligned}
& (-\sqrt{2}, -\sqrt{2}, -\sqrt{2}, -\sqrt{2}, 0, 0, 0, 0), (-\sqrt{2}, -\sqrt{2}, \sqrt{2}, \sqrt{2}, 0, 0, 0, 0), \\
& (-\sqrt{2}, \sqrt{2}, -\sqrt{2}, \sqrt{2}, 0, 0, 0, 0), (-\sqrt{2}, \sqrt{2}, \sqrt{2}, -\sqrt{2}, 0, 0, 0, 0), \\
& (0, 0, 0, 0, -\sqrt{2}, -\sqrt{2}, -\sqrt{2}, -\sqrt{2}), (0, 0, 0, 0, -\sqrt{2}, -\sqrt{2}, \sqrt{2}, \sqrt{2}), \\
& (0, 0, 0, 0, -\sqrt{2}, \sqrt{2}, -\sqrt{2}, \sqrt{2}), (0, 0, 0, 0, -\sqrt{2}, \sqrt{2}, \sqrt{2}, -\sqrt{2}),
\end{aligned}$$

$$\begin{aligned}
& (0, 0, 0, 0, \sqrt{2}, -\sqrt{2}, -\sqrt{2}, \sqrt{2}), (0, 0, 0, 0, \sqrt{2}, -\sqrt{2}, \sqrt{2}, -\sqrt{2}), \\
& (0, 0, 0, 0, \sqrt{2}, \sqrt{2}, -\sqrt{2}, -\sqrt{2}), (0, 0, 0, 0, \sqrt{2}, \sqrt{2}, \sqrt{2}, \sqrt{2}), \\
& (\sqrt{2}, -\sqrt{2}, -\sqrt{2}, \sqrt{2}, 0, 0, 0, 0), (\sqrt{2}, -\sqrt{2}, \sqrt{2}, -\sqrt{2}, 0, 0, 0, 0), \\
& (\sqrt{2}, \sqrt{2}, -\sqrt{2}, -\sqrt{2}, 0, 0, 0, 0), (\sqrt{2}, \sqrt{2}, \sqrt{2}, \sqrt{2}, 0, 0, 0, 0).
\end{aligned}$$

Consequently, if  $n$  is even,  $f \oplus s_8, f \oplus s_2 \oplus s_8, f \oplus s_4 \oplus s_8, f \oplus s_2 \oplus s_4 \oplus s_8$  are all bent with the conditions that  $(W_{f \oplus s_8}(\mathbf{u}), W_{f \oplus s_8}(\bar{\mathbf{u}}), W_{f \oplus s_2 \oplus s_8}(\mathbf{u}), W_{f \oplus s_2 \oplus s_8}(\bar{\mathbf{u}}), W_{f \oplus s_4 \oplus s_8}(\mathbf{u}), W_{f \oplus s_4 \oplus s_8}(\bar{\mathbf{u}}), W_{f \oplus s_2 \oplus s_4 \oplus s_8}(\mathbf{u}), W_{f \oplus s_2 \oplus s_4 \oplus s_8}(\bar{\mathbf{u}})) = (1, 1, 1, 1, 1, 1, 1, 1) \star (-1)^\ell$ , where  $\ell \in \mathcal{A}_3$ , and  $\mathcal{A}_3$  are the affine functions in three variables.

If  $n$  is odd, then  $f \oplus s_8, f \oplus s_2 \oplus s_8, f \oplus s_4 \oplus s_8, f \oplus s_2 \oplus s_4 \oplus s_8$  are all semibent and  $(W_{f \oplus s_8}(\mathbf{u}), W_{f \oplus s_8}(\bar{\mathbf{u}}), W_{f \oplus s_2 \oplus s_8}(\mathbf{u}), W_{f \oplus s_2 \oplus s_8}(\bar{\mathbf{u}})) = (\sqrt{2}, \sqrt{2}, \sqrt{2}, \sqrt{2}) \star (-1)^\ell$ ,  $\ell \in \mathcal{A}_2$ , and  $\mathcal{A}_2$  are the affine functions in two variables, and  $W_{f \oplus s_4 \oplus s_8}(\mathbf{u}) = W_{f \oplus s_4 \oplus s_8}(\bar{\mathbf{u}}) = W_{f \oplus s_2 \oplus s_4 \oplus s_8}(\mathbf{u}) = W_{f \oplus s_2 \oplus s_4 \oplus s_8}(\bar{\mathbf{u}})) = 0$ ; or,  $(W_{f \oplus s_4 \oplus s_8}(\mathbf{u}), W_{f \oplus s_4 \oplus s_8}(\bar{\mathbf{u}}), W_{f \oplus s_2 \oplus s_4 \oplus s_8}(\mathbf{u}), W_{f \oplus s_2 \oplus s_4 \oplus s_8}(\bar{\mathbf{u}})) = (\sqrt{2}, \sqrt{2}, \sqrt{2}, \sqrt{2}) \star (-1)^\ell$ ,  $\ell \in \mathcal{A}_2$ , and  $W_{f \oplus s_8}(\mathbf{u}) = W_{f \oplus s_8}(\bar{\mathbf{u}}) = W_{f \oplus s_2 \oplus s_8}(\mathbf{u}) = W_{f \oplus s_2 \oplus s_8}(\bar{\mathbf{u}}) = 0$ .

It is a simple computation to check that these values of the Walsh-Hadamard coefficients will render  $f$  hexabent, and so, the reciprocal is true, as well.  $\square$

**Corollary 11.** *If  $f$  is octabent,  $\zeta = e^{\frac{2\pi}{16}}$ , then the hexa-Hadamard spectrum of  $f$  is  $\{\zeta^k \mid 0 \leq k \leq 15\}$ . If  $f$  is weak hexabent then its spectrum in absolute value belongs to a 32 element set.*

*Proof.* The proof is a straightforward computation running through the set of values for the Walsh-Hadamard coefficients described in the previous theorem, respectively all  $\pm 1$  Walsh-Hadamard coefficients and removing duplicates, for the second claim.  $\square$

## 4 The general case of $2^k$ -bent functions

As in the case of negabent functions, one can characterize the  $2^k$ -bent functions in terms of codimension one subspace decomposition. We write  $\Re(z), \Im(z)$  for the real part, respectively, imaginary part of a complex number  $z$ .

**Theorem 12.** *Let  $h \in \mathcal{B}_n$  and  $h(\mathbf{x}, y) = f(\mathbf{x})(1 \oplus y) \oplus y g(\mathbf{x})$ . Then  $f$  is  $2^k$ -bent if and only if  $|H_f(\mathbf{u})|^2 + |H_g(\mathbf{u})|^2 = 2$  and  $\Re(\zeta) \Re(\mathcal{H}_f(\mathbf{u}) \overline{\mathcal{H}_g(\mathbf{u})}) + \Im(\zeta) \Im(\mathcal{H}_f(\mathbf{u}) \overline{\mathcal{H}_g(\mathbf{u})}) = 0$ .*

*Proof.* We first find the  $2^k$ -Hadamard transform of  $f$ ,

$$\begin{aligned}
\mathcal{H}_h(\mathbf{x}, y) &= 2^{-\frac{n+1}{2}} \sum_{\substack{\mathbf{u} \in \mathbb{V}_n \\ v \in \mathbb{F}_2}} (-1)^{h(\mathbf{u}, v) \oplus \mathbf{u} \cdot \mathbf{x} \oplus vy} \zeta^{\text{wt}(\mathbf{u}) + v} \\
&= 2^{-\frac{n+1}{2}} \sum_{\mathbf{u} \in \mathbb{V}_n} (-1)^{f(\mathbf{u}) \oplus \mathbf{u} \cdot \mathbf{x}} \zeta^{\text{wt}(\mathbf{u})} \\
&\quad + 2^{-\frac{n+1}{2}} \zeta(-1)^y \sum_{\mathbf{u} \in \mathbb{V}_n} (-1)^{g(\mathbf{u}) \oplus \mathbf{u} \cdot \mathbf{x}} \zeta^{\text{wt}(\mathbf{u})} \\
&= \frac{1}{\sqrt{2}} \mathcal{H}_f(\mathbf{u}) + \frac{1}{\sqrt{2}} \zeta(-1)^y \mathcal{H}_g(\mathbf{u}).
\end{aligned}$$

Taking complex norms (with notations  $\zeta = \alpha + i\beta$ ,  $\mathcal{H}_f(\mathbf{u}) = z_1 + iz_2$ ,  $\mathcal{H}_g(\mathbf{u}) = w_1 + iw_2$ ), squaring and simplifying the expressions, we get

$$\begin{aligned}
2|\mathcal{H}_h(\mathbf{x}, 0)|^2 &= |\mathcal{H}_f(\mathbf{u})|^2 + |\mathcal{H}_g(\mathbf{u})|^2 + 2\alpha(z_1w_1 + z_2w_2) + 2\beta(w_1z_2 - z_1w_2) \\
2|\mathcal{H}_h(\mathbf{x}, 1)|^2 &= |\mathcal{H}_f(\mathbf{u})|^2 + |\mathcal{H}_g(\mathbf{u})|^2 - 2\alpha(z_1w_1 + z_2w_2) - 2\beta(w_1z_2 - z_1w_2).
\end{aligned}$$

If  $h$  is  $2^k$ -bent, then we immediately get (by adding the above expressions) that  $|\mathcal{H}_f(\mathbf{u})|^2 + |\mathcal{H}_g(\mathbf{u})|^2 = 2$ , and  $\alpha(z_1w_1 + z_2w_2) = \beta(w_2z_1 - z_2w_1)$ . The reciprocal is also true and the theorem is shown.  $\square$

It turns out that we can prove that the bent ladder we previously observed is preserved (we shall be more precise below), although, we are only able to show a sufficiency criterion. Let  $\mathcal{L}_{k-1}$  be the set of all linear functions in  $k-1$  variables and let  $\Psi := (1, \zeta, \dots, \zeta^{2^{k-1}})$ .

**Theorem 13.** *Let  $f \in \mathcal{B}_n$  and  $k \geq 3$ . The  $2^k$ -Hadamard transform and  $2^{k-1}$ -Hadamard transforms are related by*

$$2^{k-1} \mathcal{H}_f^{(2^k)}(\mathbf{u}) = \sum_{\ell_{\mathbf{a}} \in \mathcal{L}_{k-1}} \beta_{\mathbf{a}} W_{f \oplus s_{2^{k-1}} \oplus \sum_{j=0}^{k-2} \epsilon_j s_{2^j}}(\mathbf{u}), \quad (5)$$

where  $\ell_{\mathbf{a}} = \sum_{j=0}^{n-1} \epsilon_j x_j \in \mathcal{L}_{k-1}$ , for  $\epsilon_j \in \{0, 1\}$ , and  $\beta_{\mathbf{a}} = \Psi \cdot (-1)^{\ell_{\mathbf{a}}}$ . Moreover, if  $n$  is even and all  $f \oplus s_{2^{k-1}} \oplus \sum_{j=0}^{k-2} \epsilon_j s_{2^j}$  are bent with their Walsh-Hadamard transforms' signs matching the character forms of the linear functions in  $k-1$  variables, then  $f$  is  $2^k$ -bent. If  $n$  is odd and all  $f \oplus \sum_{j=1}^{k-1} \epsilon_j s_{2^j}$  are semibent, with the extra condition that either the Walsh-Hadamard transforms of  $f \oplus s_{2^{k-1}} \oplus \sum_{j=0}^{k-3} \epsilon_j s_{2^j}$  match the signs of the linear functions in  $k-2$  variables, and the rest of the  $2^{k-2}$  Walsh-Hadamard transforms of  $f \oplus s_{2^{k-1}} \oplus s_{2^{k-2}} \oplus \sum_{j=0}^{k-3} \epsilon_j s_{2^j}$  are zero, or vice-versa, then  $f$  is  $2^k$ -bent.

*Proof.* By Lemma 5, we compute (we let  $\zeta := \zeta_{2^k}$ )

$$\begin{aligned}
2^{k-1} \mathcal{H}_f^{(2^k)}(\mathbf{u}) &= 2^{-\frac{n}{2}+k-1} \sum_{\mathbf{x} \in \mathbb{V}_n} (-1)^{f(\mathbf{x}) \oplus \mathbf{u} \cdot \mathbf{x}} \zeta^{\text{wt}(\mathbf{x})} \\
&= 2^{-\frac{n}{2}+k-1} \sum_{\mathbf{x} \in \mathbb{V}_n} (-1)^{f(\mathbf{x}) \oplus s_{2^k-1}(\mathbf{x}) \oplus \mathbf{u} \cdot \mathbf{x}} \zeta^{s_1(\mathbf{x}) \oplus 2s_2(\mathbf{x}) \oplus \dots \oplus s_{2^k-1}(\mathbf{x})} \\
&= 2^{-\frac{n}{2}} \sum_{\mathbf{x} \in \mathbb{V}_n} (-1)^{f(\mathbf{x}) \oplus s_{2^k-1}(\mathbf{x}) \oplus \mathbf{u} \cdot \mathbf{x}} \left( (1 + \zeta) + (1 - \zeta)(-1)^{s_1(\mathbf{x})} \right) \\
&\quad \cdot \left( (1 + \zeta^2) + (1 - \zeta^2)(-1)^{s_2(\mathbf{x})} \right) \\
&\quad \cdot \left( (1 + \zeta^4) + (1 - \zeta^4)(-1)^{s_4(\mathbf{x})} \right) \dots \\
&\quad \cdot \left( (1 + \zeta^{2^{k-1}}) + (1 - \zeta^{2^{k-1}})(-1)^{s_{2^k-1}(\mathbf{x})} \right)
\end{aligned}$$

which, by expansion, renders our first claim.

Now, if we consider all  $f \oplus \sum_{j=1}^{k-1} \epsilon_j s_{2^j}$  bent with the Walsh-Hadamard transforms having the signs of the character forms of some linear function in  $k-1$  variables, say  $\ell_{\mathbf{b}} \in \mathcal{L}_{k-1}$ , then we see that the right hand side of equation (5) becomes

$$\begin{aligned}
2^{k-1} \mathcal{H}_f^{(2^k)}(\mathbf{u}) &= (\beta_{\mathbf{a}})_{\ell_{\mathbf{a}} \in \mathcal{L}_{k-1}} \cdot (-1)^{\ell_{\mathbf{b}}} \\
&= \Psi \cdot (-1)^{\ell_{\mathbf{a}} \oplus \ell_{\mathbf{b}}} = \sum_{\mathbf{a}} \beta_{\mathbf{a}} = 2^{k-1},
\end{aligned}$$

since multiplying by  $(-1)^{\ell_{\mathbf{b}}}$  has the effect of permuting the sum of  $\beta_{\mathbf{a}}$ , and moreover, every coefficient of  $\zeta^i$ ,  $i \geq 1$ , has the same number of  $\pm 1$  in such a sum. A similar argument holds for  $n$  odd. The proof is done.  $\square$

We challenge the community to construct classes of weak and strong  $2^k$ -bent functions or show that they do not exist for various values of  $k$ .

## References

- [1] C. Carlet, Boolean functions for cryptography and error correcting codes. In: Y. Crama, P. Hammer (eds.), Boolean Methods and Models, Cambridge Univ. Press, Cambridge. Available: <http://www-roc.inria.fr/secret/Claude.Carlet/pubs.html>.

- [2] C. Carlet, Vectorial Boolean functions for cryptography. In: Y. Crama, P. Hammer (eds.), *Boolean Methods and Models*, Cambridge Univ. Press, Cambridge. Available: <http://www-roc.inria.fr/secret/Claude.Carlet/pubs.html>.
- [3] T.W. Cusick, P. Stănică, *Cryptographic Boolean functions and Applications*, Elsevier–Academic Press, 2009.
- [4] S. Gangopadhyay, E. Pasalic, P. Stănică, *A note on generalized bent criteria for Boolean functions*, IEEE Trans. Inf. Theory 59:5 (2013), 3233–3233.
- [5] F. J. MacWilliams, N. J. A. Sloane, *The theory of error correcting codes*, North-Holland, Amsterdam, 1977.
- [6] T. Martinsen, W. Meidl, P. Stănică, *Generalized partial spread Boolean functions*, manuscript, 2015.
- [7] M. G. Parker, A. Pott, *On Boolean functions which are bent and negabent*. In: S.W. Golomb, G. Gong, T. Helleseth, H.-Y. Song (eds.), SSC 2007, LNCS 4893 (2007), Springer, Heidelberg, 9–23.
- [8] C. Riera, M. G. Parker, *One and two-variable interlace polynomials: A spectral interpretation*, Proc. of WCC 2005, LNCS 3969 (2006), Springer, Heidelberg, 397–411.
- [9] C. Riera, M. G. Parker, *Generalized bent criteria for Boolean functions*, IEEE Trans. Inf. Theory 52:9 (2006), 4142–4159.
- [10] O.S. Rothaus, *On “bent” functions*, J. Combin. Theory Ser. A 20 (1976), 300–305.
- [11] P. Stănică, S. Gangopadhyay, A. Chaturvedi, A.K. Gangopadhyay, S. Maitra, *Investigations on bent and negabent functions via the nega-Hadamard transform*, IEEE Trans. Inf. Theory 58 (2012), 4064–4072.
- [12] W. Su, A. Pott, X. Tang, *Characterization of Negabent Functions and Construction of Bent-Negabent Functions With Maximum Algebraic Degree*, IEEE Trans. Inf. Theory 59:6 (2013), 3387–3395.